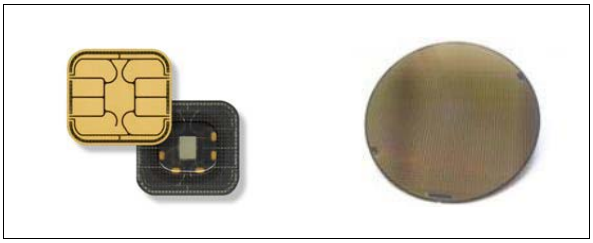
ST33G1M2SM, ST33GxxxSM

Secure MCU with 32-bit ARM® SecurCore® SC300™ CPU, MIFARE®, SWP, ISO, SPI, GPIO interface and high-density Flash memory

Data brief



Features

Hardware features

- ARM® SecurCore® SC300™ 32-bit RISC core cadenced at 25 MHz
- 30 Kbytes of User RAM
- Up to 1280 Kbytes of User Flash memory with OTP area
- Asynchronous receiver transmitter supporting ISO/IEC 7816-3 T=0 and T=1 protocols (Slave mode supported)
- Single Wire Protocol (SWP) Interface for communications with NFC router (ETSI 102-613 compliant)
- Serial peripheral interface (SPI) master/slave interface
- Three 16-bit timers with interrupt capability
- Seven general purpose I/Os enabling proprietary protocol implementation
- 1.8 V, 3 V and 5 V supply voltage ranges
- External clock frequency from 1 up to 10 MHz
- Current consumption compatible with GSM and ETSI specifications
- Power-saving standby state
- Contact assignment compatible with ISO/IEC 7816-2
- ESD protection greater than 4 kV (HBM)

Software features

- MIFARE® libraries[a]: MIFARE® Classic, MIFARE DESFire® EV1
- Secure Flash Loader
- Flash drivers

Security features

- MIFARE® Classic cryptography hardware accelerator
- Active shield
- Memory protection unit (MPU)
- Monitoring of environmental parameters
- Protection against faults
- 16- and 32-bit CRC calculation block (ISO 13239, IEEE 802.3, etc.)
- True random number generator
- Unique serial number on each die
- Hardware security-enhanced DES accelerator
- Hardware security-enhanced AES accelerator
- NESCRYPT coprocessor for public key cryptography algorithm

Applications

ST33G1M2SM[b] major applications include:

- Mobile communications (GSM, 3G and CDMA)
- Automatic Fare Collection (included Transport & Event ticketing, Loyalty programs)
- Java Card applications
- Multimedia

Table 1. Device summary

Part number	Flash (Kbytes)
ST33G1M2SM	1280
ST33G1M0SM	1024
ST33G896SM	896
ST33G768SM	768
ST33G640SM	640
ST33G512SM	512

a. MIFARE, MIFARE Classic, MIFARE DESFire are trademarks of NXP B.V. and are used under license.

b. ST33G1M2SM* is the master product that refers to all commercial derivatives summarized in *Table 1*.

1 Description

The ST33G1M2SM is a serial access microcontroller designed for secure mobile applications that incorporates the most recent generation of ARM® processors for embedded secure systems. Its SecurCore® SC300™ 32-bit RISC core is built on the Cortex® M3 core with additional security features to help to protect against advanced forms of attacks.

The SC300™ core brings great performance and excellent code density thanks to the Thumb®-2 instruction set.

The high-speed embedded Flash memory introduces more flexibility to the system.

The ST33G1M2SM also offers a serial communication interface fully compatible with the ISO/IEC 7816-3 standard (T=0, T=1) and a single-wire protocol (SWP) interface for communication with a near field communication (NFC) router in SIM/NFC applications.

The ST33G1M2SM embeds a MIFARE® Library fully compatible with the widely deployed MIFARE® Classic and MIFARE DESFire® EV1 contactless scheme. Both MIFARE® Classic and MIFARE DESFire® EV1 can be used in mobile contactless applications such as Transport & Event ticketing, Access Control, Loyalty programs.

An SPI Master/Slave interface is also available for communication in non-SIM applications.

The ST33G1M2SM features hardware accelerators for advanced cryptographic functions. The EDES peripheral provides a secure DES (Data Encryption Standard) algorithm implementation, while the NESCRYPT crypto-processor efficiently supports the public key algorithm. The AES peripheral ensures secure and fast AES algorithm implementation.

The ST33G family operates in the –25 to +85°C temperature range and 1.8V, 3V and 5V supply voltage ranges. A comprehensive range of power-saving modes enables the design of efficient low-power applications.

Software development tools description

Dedicated SecurCore® SC300™ software development tools are provided by ARM and Keil. This includes the Instruction Set Simulator (ISS) and C compiler. The documentation is available on the ARM and Keil web sites.

Moreover, STMicroelectronics provides:

- A time-accurate hardware emulator controlled by the Keil debugger and the STMicroelectronics development environment.
- A complete product simulator based on Keil's ISS simulator for the SecurCore® SC300™ CPU.
- A secured ROMed Flash Loader with very high-speed software downloading capabilities.

Note: For MIFARE library usage, please, refer to the ST33G Firmware user manual*.*

2 Revision history

Table 2. Document revision history

Date	Revision	Changes
26-Jun-2914	1	Initial release.

Please Read Carefully:

Information in this document is provided solely in connection with ST products. STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, modifications or improvements, to this document, and the products and services described herein at any time, without notice.

All ST products are sold pursuant to ST’s terms and conditions of sale.

Purchasers are solely responsible for the choice, selection and use of the ST products and services described herein, and ST assumes no liability whatsoever relating to the choice, selection or use of the ST products and services described herein.

No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted under this document. If any part of this document refers to any third party products or services it shall not be deemed a license grant by ST for the use of such third party products or services, or any intellectual property contained therein or considered as a warranty covering the use in any manner whatsoever of such third party products or services or any intellectual property contained therein.

UNLESS OTHERWISE SET FORTH IN ST’S TERMS AND CONDITIONS OF SALE ST DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE USE AND/OR SALE OF ST PRODUCTS INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE (AND THEIR EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION), OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

ST PRODUCTS ARE NOT DESIGNED OR AUTHORIZED FOR USE IN: (A) SAFETY CRITICAL APPLICATIONS SUCH AS LIFE SUPPORTING, ACTIVE IMPLANTED DEVICES OR SYSTEMS WITH PRODUCT FUNCTIONAL SAFETY REQUIREMENTS; (B) AERONAUTIC APPLICATIONS; (C) AUTOMOTIVE APPLICATIONS OR ENVIRONMENTS, AND/OR (D) AEROSPACE APPLICATIONS OR ENVIRONMENTS. WHERE ST PRODUCTS ARE NOT DESIGNED FOR SUCH USE, THE PURCHASER SHALL USE PRODUCTS AT PURCHASER’S SOLE RISK, EVEN IF ST HAS BEEN INFORMED IN WRITING OF SUCH USAGE, UNLESS A PRODUCT IS EXPRESSLY DESIGNATED BY ST AS BEING INTENDED FOR “AUTOMOTIVE, AUTOMOTIVE SAFETY OR MEDICAL” INDUSTRY DOMAINS ACCORDING TO ST PRODUCT DESIGN SPECIFICATIONS. PRODUCTS FORMALLY ESCC, QML OR JAN QUALIFIED ARE DEEMED SUITABLE FOR USE IN AEROSPACE BY THE CORRESPONDING GOVERNMENTAL AGENCY.

Resale of ST products with provisions different from the statements and/or technical features set forth in this document shall immediately void any warranty granted by ST for the ST product or service described herein and shall not create or extend in any manner whatsoever, any liability of ST.

ST and the ST logo are trademarks or registered trademarks of ST in various countries.
Information in this document supersedes and replaces all information previously supplied.
The ST logo is a registered trademark of STMicroelectronics. All other names are the property of their respective owners.

© 2014 STMicroelectronics - All rights reserved

STMicroelectronics group of companies

Australia - Belgium - Brazil - Canada - China - Czech Republic - Finland - France - Germany - Hong Kong - India - Israel - Italy - Japan - Malaysia - Malta - Morocco - Philippines - Singapore - Spain - Sweden - Switzerland - United Kingdom - United States of America

www.st.com